

1/6

10
12 {
14 }
24 {
26 {
sessionid=123ashg&id=7654, HTTP/1.1 }
16 {
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-e
Referer: http://www.cnn.com/
18 {
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; T312461)
20 {
Cookie: CNNid=Gcf1947e6-25267-997291842-7; NGUserID=cf1947bf-8936-998251970-1; bi
Host: www.cnn.com
Connection: Keep-Alive
20 }

FIG. 1A

2/6

POST /cgi-bin/acnotify.cgi HTTP/1.1
 {
 Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/msword, application/vnd.ms-powerpoint, */*
 Referer: http://mobile.aircanada.ca/aircanada/notify.shtml
 Accept-Language: en-us
 Content-Type: application/x-www-form-urlencoded → 18a'
 Accept-Encoding: gzip, deflate
 User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; T312461)
 Host: mobile.airline.ca
 Content-Length: 125
 20' {Cookie: new_lang_pref=english
 Connection: Keep-Alive
 18' {Cache-Control: no-cache → 25:
 24' { lang = en&format = html&action = confirm&fn = 5454&fdate = 2002-09-
 22' { 06&ad = d&dt = 15&athb = 1&devtype = e&dev = none&phone = joe.smith@sympatico.ca

FIG. 1B

3/6

12" → 14" → 16" → 10"

POST /bookingform.jsp HTTP/1.1

18a" { Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/msword, application/vnd.ms-powerpoint, */*

18" { Accept-Language: en-us
Content-Type: multipart/form-data; boundary = -----
7d23403440456
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; T312461)
Host: scan.airline.ca
Content-Length: 150
Connection: Keep-Alive
Cache-Control: no-cache
----- 7d23403440456 ← 30" 28"
Content-Disposition: form-data; name = "phone"
(416) 841-7712 24" 26"
----- 7d23403440456
Content-Disposition: form-data; name = "passengers"
22" { 2
----- 7d23403440456
Content-Disposition: form-data; name = "comment"
vegetarian meal only
----- 7d23403440456--

FIG. 1C

4/6

POST /StockQuote HTTP/1.1
Host: www.stockquoteserver.com
Content-Type: text/xml; charset = "utf-8"
Content-Length: nnnn
SOAPAction: "Some-URI"

< SOAP-ENV:Envelope
 xmlns:SOAP-ENV = "http://schemas.xmlsoap.org/soap/envelope/"
 SOAP-ENV:encodingStyle = "http://schemas.xmlsoap.org/soap/
 encoding/" />
< SOAP-ENV:Header >
 < t:Transaction xmlns:t = "some-URI" SOAP-
 ENV:mustUnderstand = "1" >
 5
 < /t:Transaction >
 </SOAP-ENV:Header >
< SOAP-ENV:Body >
 < m:GetLastTradePriceDetailed xmlns:m = "Some-URI" >
 < Symbol > DEF < /Symbol >
 < Company > DEF Corp < /Company >
 25" < Price > 34.1 < /Price >
 < /m:GetLastTradePriceDetailed >
< /SOAP-ENV:Body >
< /SOAP-ENV:Envelope >

FIG. 1D

5/6

50

Trigger: All request for URLs containing the characters "form"

Conditions:

- The method must be POST 54 56
- There must exist between 1 and 100 POST fields 54
- No more than 5% of the POST fields may have blank (empty) values 58
- There must exist exactly one field named Comments
- The value of the Comments field must be between 20 and 2000 characters in length
- The statistical distribution of characters in the Comments field must not differ from that of standard English by more than the threshold X

Trigger: All request for URLs ending in the characters ".jsp"

Conditions:

- There must exist exactly one cookie named SessionID 56
- There may not exist any cookies not named SessionID
- The value of the SessionID cookie must be between 12 and 14 characters in length and must be composed exclusively of the numerals 0 through 9 and the uppercase letters A through F
- The method must be HEAD or GET

Trigger: All request for URLs beginning with the characters "/images"

OR ending with the characters ".gif" or ".jpg"

Conditions:

- The method must be HEAD or GET
- There must not be any GET parameters
- There must not be any cookies
- There must be no more than ten headers
- The URI must not exceed 200 characters in length

FIG. 2

6/6

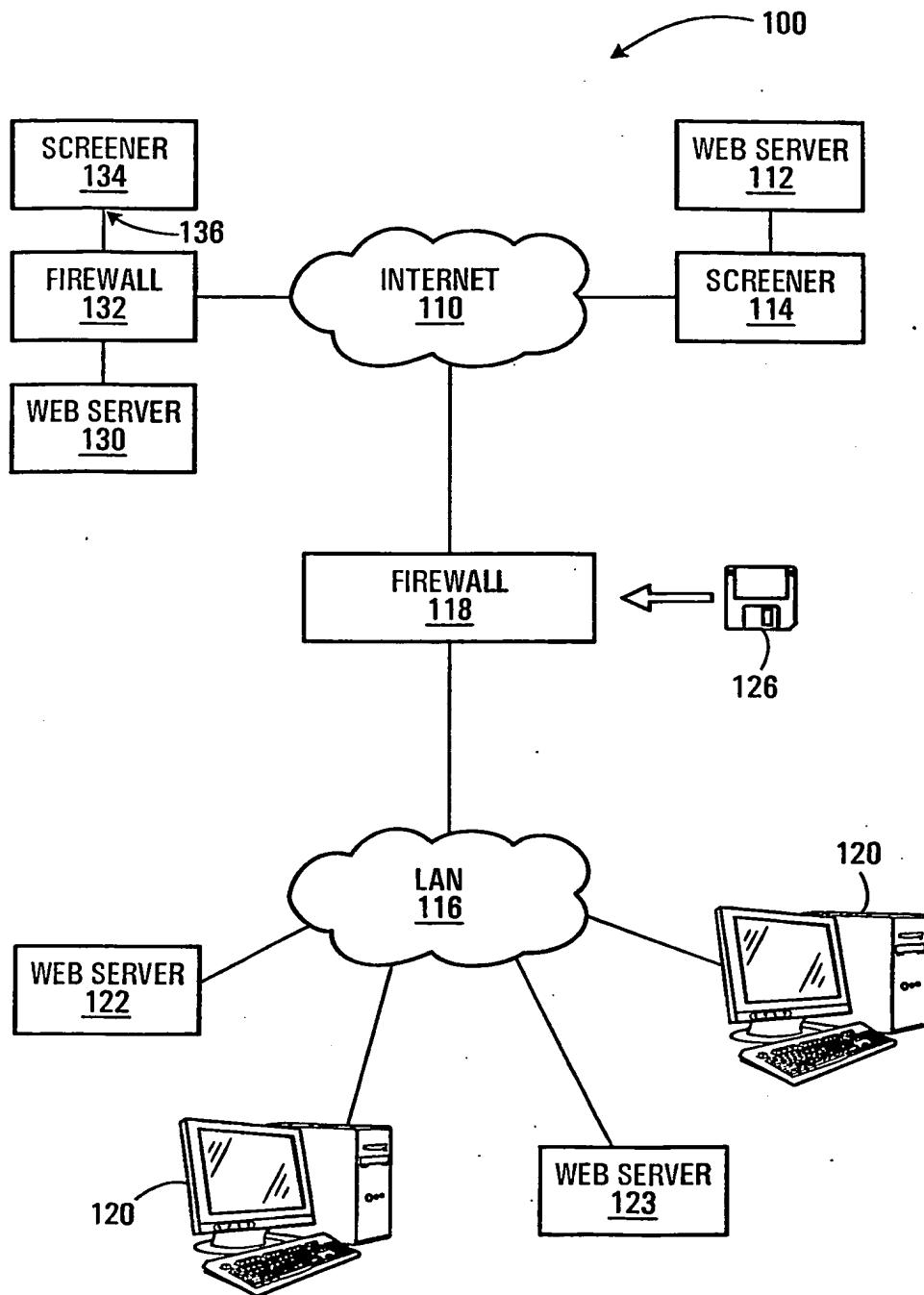


FIG. 3